UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/607,412 | 06/29/2000 | Howard C. Herbert | 042390.P7704 | 7770 |

7590 01/21/2004

William W Schaal
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

| EXAMINER | |
|---|---|
| VAUGHAN, MICHAEL R | |
| ART UNIT | PAPER NUMBER |
| 2131 | |

DATE MAILED: 01/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/607,412 | HERBERT ET AL. | |
| | Examiner | Art Unit | |
| | Michael R Vaughan | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *29 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

## DETAILED ACTION

1. Claims 1-41 have been examined and are pending.

### *Claim Rejections - 35 USC ' 112, second paragraph*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 27-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear as to what merits the distinction of the first part and second part of (BEKp2) bundles. Clarification and/or correction are required.

### *Claim Rejections - 35 USC ' 112, first paragraph*

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 27-32 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the

application was filed, had possession of the claimed invention. The specification discloses the use of (BEKp1) and (BEKp2) as being the first and second parts of the bundle encryption key, respectively. Claims 27-32 reference (BEKp2) as being both parts of the encryption key.

***Claim Rejections - 35 USC ' 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

> the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1-9, 17, 21-34, 37-39, and 41 are rejected under 35 U.S.C. 102(a) as being anticipated by Yamazaki et al (JP 11298470 A).

As per claim 1, Yamazaki et al teach:

storing a current sort encryption key (SEK) at a first destination in an internal memory of an electronic component (see paragraph [0006]);

storing a next SEK at the first destination in the internal memory [0006];

providing the electronic component to a second destination [0005]; and

recovering a private key at the second destination from a key bundle based

on the current SEK, the next SEK and a plurality of bundles received at the second destination [0008].

As per claim 17, Yamazaki et al teach a method comprising:

at a first destination, recovering a current sort encryption key (SEK) and a next SEK based on information within a first plurality of incoming bundles [0024] and

storing the current SEK and the next SEK in an internal memory of an electronic component [0025], [0051]; and

at a second destination, upon receipt of the electronic component,

recovering a private key from a key bundle based on the current SEK, the next SEK and a second plurality of incoming bundles [0059].

As per claim 2, transferring at least a first bundle to the first destination via a first link [0007]; and

transferring at least a second bundle to the first destination via a first out of-band information carrying mechanism [0007].

As per claims 3 and 21, Yamazaki et al teach the first bundle includes a plurality of configuration window (CWIN) bundles [0005].

As per claims 4 and 22, Yamazaki et al teach each of the CWIN bundles includes a configuration window material, the configuration window includes

(i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated. with the next SEK, (iv) the next SEK and (v) a group integrity check value for a first encryption key and a second encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claims 5 and 23, Yamazaki et al teach wherein the configuration window material

is encrypted with the first encryption key and the second encryption key [0008].

As per claims 6 and 24, Yamazaki et al teach each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key [0006].

As per claims 7 and 25, Yamazaki et al teach the second bundle includes a plurality of sort encryption key (SEK) bundles [0060].

As per claims 8 and 26, Yamazaki et al teach each of the SEK bundles includes

(i) a sort encryption key, (ii) a key identifier associated with the sort encryption key and (iii) an integrity check value associated with the sort encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claim 9, Yamazaki et al teach transferring the plurality of bundles to the second destination, the plurality of bundles includes a third bundle and a fourth bundle [0060].

As per claims 27, Yamazaki et al teach the second plurality of bundles includes a plurality of first part bundle encryption key (BEKp2) bundles and a plurality of second part bundle encryption key (BEKP2) bundles [0008].

As per claim 28, Yamazaki et al teach each of the BEKp2 bundles includes a second part of the bundle encryption key and a group integrity check value for a first encryption key and a second encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claims 29, Yamazaki et al teach one of the BEKp2 bundles includes a first part of the bundle encryption key and an integrity check value associated with the current SEK [0022].

As per claim 30, Yamazaki et al teach one of the BEKp2 bundles includes a first part of the bundle encryption key and an integrity check value associated with the next SEK [0022].

As per claim 31, Yamazaki et al teach the bundle encryption key is recovered upon recovering the first and second parts of the bundle encryption key [0051].

As per claim 32, Yamazaki et al teach the private key is recovered using the bundle encryption key [0051].

As per claim 33, Yamazaki et al teach a method comprising:

receiving at least a first bundle via a first link [0007];

receiving at least a second bundle via a first out-of-band information carrying mechanism [0007];

recovering a current sort encryption key (SEK) and a next SEK based on information contained in the first bundle and the second bundle [0051]; and

storing the current SEK and the next SEK in an internal memory of an electronic component [0022].

As per claim 34, Yamazaki et al teach transferring the electronic component to a second destination [0005].

As per claim 37, Yamazaki et al teach a source to output a first collection of encrypted keying material and a second collection of encrypted keying material [0006];

a first destination to receive the first collection of encrypted keying material, to decrypt keying material originating from the first collection of encrypted keying material

for recovery of sort encryption keying material and to store the sort encryption keying material into an internal memory of an electronic component [0005]; and

a second destination to receive the second collection of encrypted keying material, to decrypt keying material originating from the second collection of encrypted keying material for recovery of at least private key for subsequent loading in the internal memory [0005-0008].

As per claim 38, Yamazaki et al teach wherein the first destination is physically separated from the second destination [0006].

As per claim 39, Yamazaki et al teach wherein the sort encryption keying material includes a current sort encryption key (SEK) and a next SEK [0006].

As per claim 41, Yamazaki et al teach the second destination further recovers a digital certificate chain from the second collection of keying material and loads the digital certificate chain into the internal memory [0049].

***Claim Rejections - 35 USC ' 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 10-16, 35, and 36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki et al.

As per claims 10, 11, and 35, Yamazaki et al are silent in expressly the third bundle is transferred to the second destination via a second link, and that the fourth bundle is transferred to the second destination via a second out-of-band information carrying medium. Yamazaki teaches that multiple bundles are transferred to the destination over at least to channels, one in band, and one out of band [0060]. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamazaki et al by having additional

bundles exceeding the first two taught by Yamazaki et al, to also travel along the same communication channels.

As per claim 12, Yamazaki et al teach the third bundle is a plurality of second part bundle encryption key (BEKp2) bundles, each of the (BEKp2) bundles includes a second part of the bundle encryption key and a combined integrity check value associated with a first encryption key and a second encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claim 13, Yamazaki et al teach the second part of the bundle encryption key and the combined integrity check value are encrypted with the first encryption key and the second encryption key [0008].

As per claim 14, Yamazaki et al teach each BEKp2 bundle further includes a group identifier associated with the first encryption key and the second encryption key [0006].

As per claim 15, Yamazaki et al teach the fourth bundle includes a plurality of configuration encryption key (CEK) bundles [0005].

As per claim 16, Yamazaki et al teach each of the CEK bundles includes (i) a configuration encryption key, (ii) a key identifier associated with the configuration

encryption key and (iii) an integrity check value associated with the configuration encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claim 36, Yamazaki et al teach recovering a private key based on the bundle encryption key [0008].

6. Claims 18-20 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki et al in view of Schneier (Applied Cryptography).

As per claims 18-20 and 40, Yamazaki et al are silent in expressly disclosing that a period of validity is associated with the current SEK and that when the time of validity expires, the private key is not recovered. The use of a timestamps associated with a private key is taught by Schneier (pgs. 60-61). The timestamp prevents replay attacks by an intruder to gain unprivileged information. It would be advantageous to use a timestamp in a key exchange protocol. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Schneier within the system of Yamazaki et al because it would make the system more secure by reducing the chance of replay attacks by an intruder.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

Emmanuel L. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
AU 2136